

CLAIMS

What is claimed is:

- 1 1. A method of providing secure communication between a remote
2 system and a remotely accessed system, comprising:
3 calculating at the remote system a first hash of an operation using a hash
4 algorithm;
5 encrypting at the remote system the first hash to form a signed hash;
6 receiving at the remotely accessed system the signed hash from the remote
7 system;
8 storing at the remotely accessed system a reference hash in a section of non-
9 volatile memory before receiving the signed hash;
10 validating at the remotely accessed system the signed hash using the reference
11 hash; and
12 executing at the remotely accessed system the operation associated with the
13 signed hash if the signed hash is validated.

- 1 2. The method, as set forth in claim 1, comprising responding to the
2 remote system based on the validation of the signed hash.

- 1 3. The method, as set forth in claim 2, wherein responding to the remote
2 system comprises generating a completion message if the signed hash is validated.

- 1 4. The method, as set forth in claim 2, wherein responding to the remote
2 system comprises generating an error message if the signed hash is not validated.

1 5. The method, as set forth in claim 1, wherein the operation comprises a
2 command.

1 6. The method, as set forth in claim 1, wherein the operation comprises
2 identification information.

1 7. The method, as set forth in claim 1, wherein validating comprises
2 accessing a database to access the reference hash.

1 8. The method, as set forth in claim 1, wherein validating comprises
2 parsing a packet to access the signed hash.

1 9. A method of providing secure communication between systems,
2 comprising:
3 delivering identification information to a remotely accessed system from a
4 remote system;
5 creating a nonce at the remotely accessed system;
6 delivering the nonce to the remote system;
7 calculating at the remote system a first hash of an operation using a hash
8 algorithm;
9 encrypting at the remote system the first hash along with the nonce to form a
10 signed hash;
11 receiving at the remotely accessed system the signed hash from the remote
12 system;

13 storing at the remotely accessed system a reference hash in a section of non-
14 volatile memory before receiving the signed hash;
15 validating at the remotely accessed system by comparing the signed hash to the
16 reference hash; and
17 executing at the remotely accessed system the operation associated with the
18 signed hash if the signed hash is validated.

1 10. The method, as set forth in claim 9, wherein encrypting comprises
2 signing at the remote system the first hash to form the signed hash.

1 11. The method, as set forth in claim 9, comprising parsing at the remotely
2 accessed system a packet for the first signed hash.

1 12. The method, as set forth in claim 9, comprising responding to the
2 remote system based on the validation of the signed hash.

1 13. The method, as set forth in claim 9, wherein generating the nonce at the
2 remotely accessed system comprises storing the identification information at the
3 remotely accessed system and validating comprises verifying the identification
4 information to determine if a packet is valid.

1 14. The method, as set forth in claim 9, wherein validating comprises
2 accessing a database for the reference hash, wherein the reference hash comprises a
3 second hash along with the nonce.

1 15. The method, as set forth in claim 9, wherein validating comprises
2 accessing a database for the reference hash, and combining the reference hash with the
3 nonce to validate the operation from the remote system.

1 16. The method, as set forth in claim 9, wherein validating comprises
2 verifying the identification information.

1 17. The method, as set forth in claim 9, wherein generating the nonce at the
2 remotely accessed system comprises storing the nonce at the remotely accessed system
3 and validating comprises verifying the nonce in a packet.

1 18. A system comprising:
2 a first computer system, the first computer system comprising a first program
3 for hashing information;
4 a request being generated from information received by the first computer
5 system and hashed by the first program;
6 a network connected to the first computer system and adapted to receive the
7 request;
8 a second computer system connected to the network and adapted to receive the
9 request from the first computer system, wherein the second computer system
10 comprises:
11 a processor;
12 a first section memory operatively coupled to the processor, the first
13 section memory storing a file that is a hash; and

14 a second section of memory being configured to store a validation
15 program initiated by the processor, the validation program having a validation
16 routine configured to validate the file stored in the first section of memory
17 against the received request; wherein if the received request is valid, the
18 second computer system may execute a command that corresponds to the file.

1 19. The system, as set forth in claim 18, wherein the information
2 comprises a command.

1 20. The system, as set forth in claim 19, wherein the information
2 comprises a nonce.

1 21. The system, as set forth in claim 18, wherein the first computer system
2 comprises a second program for digitally signing information.

1 22. The system, as set forth in claim 21, wherein the validation program
2 compares the hash stored in the first section of memory against signed information in
3 the received request.

1 23. The system, as set forth in claim 22, wherein the signed information
2 comprises a signed command and signed argument.